COLOSSUS

Alan Turing and the Stored Program

B. D. Price

The Turing Machine

The history of the stored program computer is too close at hand to assess properly. Astounding though it is, the modern micro would not really surprise Charles Babbage, nor Alan Turing. A hundred and fifty years ago Babbage was stymied in his plans by lack of technical skills in the mass production of gears. In 1936 Turing's approach was entirely different; being unconcerned with the practicalities of implementation he established the idea of a hypothetical machine operating on a linear sequence of binary digits; which leaves little doubt that he envisaged program and data stored together.

This so-called Turing Machine was an idea used in his paper "On Computable Numbers . .", in order to crystallise a 'definite process' as being something *capable of being done by an automatic machine.* The paper involved a proof that there do exist mathematical problems which cannot be solved by such a process. But once the idea was formed, the logical sequel was to construct such a machine, and Turing's strong interest in the experimental led to conjectures even then. He actually started building a machine to compute the Riemann Zeta-function. It is significant that Turing assumed binary numbers for his machine as being the simplest course, while not involving loss of generality.

Unfortunately Turing became heavily involved in cryptanalytic work during the last war, on which the secrecy ban has hardly been lifted. Even more unfortunate, and indeed tragic, was his death in 1954. Very little authentic material has been written on the matter. Many references in books take particular care to attribute their information to others. Randell (1) gives as comprehensive an analysis of the wartime work as possible, while skirting the issues on the borderline of secrecy. Johnson (2) has in the final stages of his book the results of research during the production of the TV series "The Secret War". This series, I have been led to believe, sailed as close to the Official Secrets Act as the BBC dared. My information is based entirely on these sources.

Enigma

Here I must digress to the topic of coding. The Germans realised in the early 30's that Blitzkrieg (lightning war) would make rapid and secure coding of wireless messages essential. To this end they adopted the Enigma machine, which was on the public market in 1923 (based on an American idea six years earlier). The machine disappeared from public view, and eventual production reached six figures (where have they all gone to?).

Any alphabetical code involves a permutation or substitution of letters by others. Enigma automatically changed the substitution at every character coded. If we apply the same sequence of substitutions to the coded message we do not in general decode a message. In order that the same machinery will code or decode as required, without any special adjustment, every substitution must be of order 2, i.e. it must exchange pairs of letters. Thus if P becomes H on coding, then H would have become P, which happens when the message is decoded. At any particular time Enigma's substitution was swopping 13 pairs of letters. This enormously reduces the number of possible substitutions from factorial 26 to approximately its square root, but these substitutions were continually changing. Nevertheless, the special properties of such substitutions gave the mathematicians, using group theory, methods of analysis.

Enigma had three rotors, each giving a random substitution of the alphabet by means of internal wiring. Depressing an alphabet key sent a current through each rotor in turn. Then one of 13 loops of wires reflected the current back through the rotors on a different path. The reflection process ensured that the overall substitution was 13 swops. Further complications introduced, as the war proceeded, were choice of rotors, and alteration of the reflecting loops by a plugboard. (The diagram on p.331 of Johnson must be incorrect — the plugboard took effect to the right of the third rotor. Also the keys must have operated changeover contacts, disconnecting the lamp and connecting to positive). The Polish Secret Service started cracking Enigma in 1928, and developed a mechanical simulation of the rotors in order to find their starting setting for any message. Just before the war they gave their knowledge to the Allies, and a series of gadgets of increasing complexity were constructed over the years, to cope with subsequent Enigma extras.

Colossus

Then the Geheimschreiber was brought into use by the Germans in 1939 or 1940 and posed a much more difficult problem. It can be examined in the Siemens Museum in Munich, and was once thought uncrackable. Two properties of this electromechanical machine are of interest here: Firstly, it operated on 5-hole teleprinter code, by altering and scrambling the binary digits. Thus cryptanalysis involved Boolean algebra. Secondly, by having ten gears with prime numbers of teeth from 47 to 89, it raised the extent of the problem to a level at which mechanical methods would have been too slow. Decoding was essentially a 'real-time' procedure. The outcome was the Colossus series of electronic computers. Several people had cracked the Geheimschreiber code by hand (though to what extent an inside knowledge of the machine helped is not divulged) and after the mathematicians, including Turing, had made the specifications the first Colossus was built, and operational in December 1943.

Colossus was the successor to several gadgets, involving Boolean algebra in valve circuitry, which were prone to mechanical errors. Colossus 1 had 1500 valves and read paper

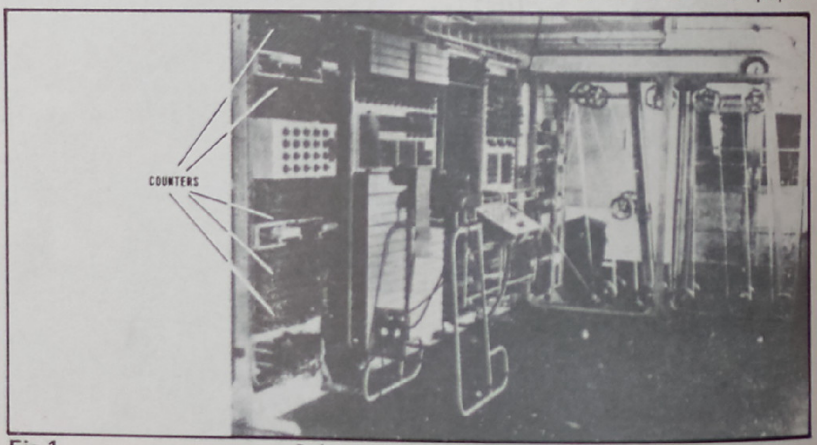

Fig 1. Colossus *(Crown Copyright)*

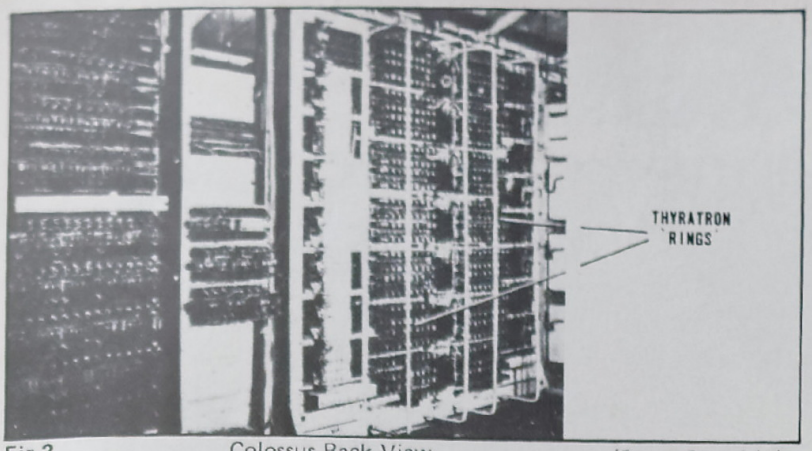

Fig 2. Colossus Back View *(Crown Copyright)*

tape at 5000 characters per second. Colossus 2 came into operation on 1 June 1944 (in time for D-day) involving about 2400 valves, and it had conditional logic incorporated. Although none of the Colossi were stored-program computers, it seems certain that Colossus 1 was the first electronic computer.

Unfortunately we have only vague information as to exactly what the Colossi were doing. Under the 'need to know' security rule people were feeding paper tape into the machines with no idea of the functions they performed. The general idea is that the coded message was being compared with a standard tape (possibly containing commonly occurring words) and Boolean functions were being counted. In some way the myriad possible setting of the prime gears were involved. At 5000 characters per second some runs took several hours. In the early devices both coded and standard messages were on tape, which gave synchronising problems, but the Colossi stored the standard message on a plugboard, and the code tape was run at high speed and provided the clock. The resulting error rate is quoted as 1 in 10^{11}.

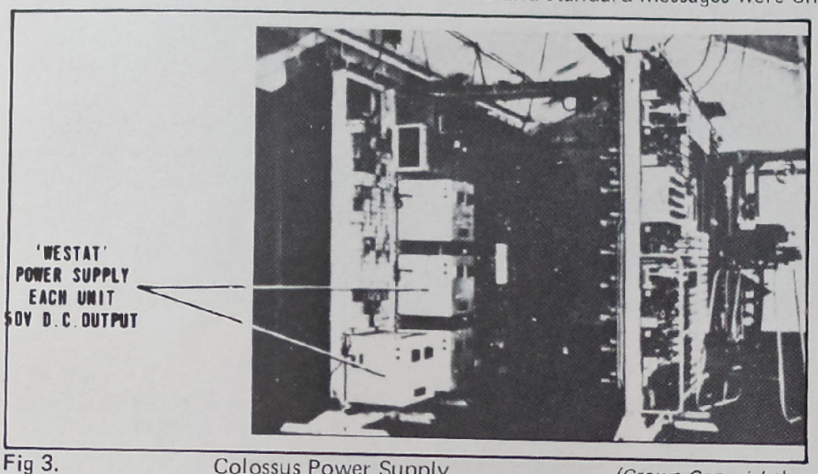

Fig 3. Colossus Power Supply *(Crown Copyright)*

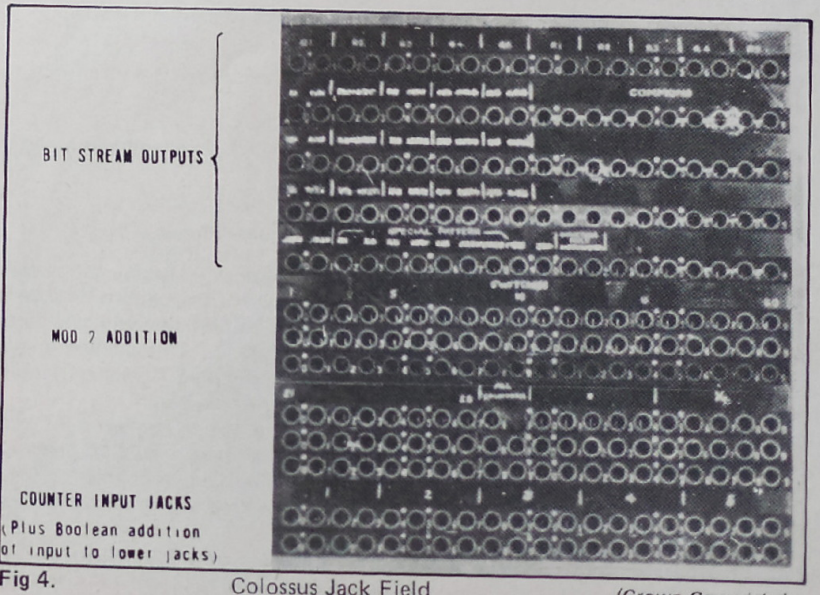

Fig 4. Colossus Jack Field *(Crown Copyright)*

In view of the well-known lectures of von Neumann in 1946 on the criteria of electronic computers, we may conjecture to what extent Turing was responsible for the underlying ideas. He paid several visits to America during the war (probably on the atomic bomb project) and must have discussed ideas on computers there. Even now it is easier to air ideas bordering on the secret in the U.S.A. than in Britain. Randell's view (1) is that von Neumann made the world aware of the fundamental concepts introduced by Turing.

Special Purpose Machines

It is interesting to compare the highly adaptable general purpose micro today, with the special purpose natures of so many historic inventions. A little-known class of special purpose mechanisms is that of the 'Change-Ringing Machines' first constructed in the 1890's by John Carter of Birmingham. His prototype of the art is in the Science Museum. My own interest in computers grew out of the mathematical problems of peal composition in change-ringing (simple ringing methods are curiously similar to the operation of Enigma) and in 1948 I corresponded with Dr. R. A. Brooker at Manchester University, who kindly attempted to solve one of my problems on their early electronic computer. Little did I know that their design staff, including Turing, came largely from the wartime operations. In 1948-1950 I constructed my own change-ringing machine from ex-government telephone relays, and I now wonder how many of the 250 relays (which I still have) were formerly in decoding gadgets! The Science Museum displays a pathetically small group of original components from Colossus.

Thus the electronic computer was born in circumstances that even now are veiled in secrecy. What a fantastic situation there was! The Germans, happy with their Enigma machine, nevertheless piled on further complexities to reassure themselves of secrecy, while in Britain mathematicians and electronics engineers strained every nerve to keep abreast of things. And then the residue of their efforts might have been sold on barrows in the Farringdon Road !

References:

(1) Professor B. Randell, "The Colossus", Technical Report Series No. 90, University of Newcastle Computing Laboratory, 1976.

(2) Brian Johnson, "The Secret War", BBC Publications 1978.